Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

IDEALS OF A QUADRATIC NUMBER FIELD IN CANONIC FORM.

By W. B. CARVER, Cornell University, Ithaca, New York.

Sommer* shows that any ideal of the quadratic field $k(\sqrt{m})$ may be reduced to a canonic form $(i,\ i_1+i_2 w)$, i, i_1, and i_2 being rational integers, i_2 a factor of both i and i_1, and

$$w\dagger=\begin{cases}\sqrt{m}, \text{ when } m \text{ is not congruent to } 1\ (4)\\ \dfrac{1+\sqrt{m}}{2}, \text{ when } m\equiv 1\ (4).\end{cases}$$

Any integer‡ of the ideal may be expressed in the form

$$li+n(i_1+i_2 w),$$

l and n being rational integers.

Using a slightly different notation, let us write the canonic form

$$r(s,\ t+w)$$

r, s, and t being rational integers, $r\neq 0$, and (to make the form unique)

$$s>t\geqq 0 \tag{1.}$$

$s=1$, $t=0$ would give the canonic form of the rational principal ideal (r), and $r=1$, $s=1$, $t=0$ would give the unit ideal containing every integer of the field.

Consider the case $r=1$, or the ideal $(s,\ t+w)$. s is the highest common factor of all the rational integers of the ideal,§ and it follows at once that t must satisfy the relation

$$\begin{cases} t^2\equiv m(s)\\ (2t+1)^2\equiv m(4s)\end{cases} \tag{2.}$$

Conversely, an ideal $(s,\ t+w)$ is in canonic form if s and t are rational in-

---

* *Vorlesungen über Zahlentheorie.* Leipzig, B. G. Teubner, 1907. See pp. 36-44. These are the ideals conceived by Dedikind and Treated by Dirichlet and others.

† Whenever double lines are written with a brace throughout this paper, the upper line will be for the case m not congruent to 1 (4) and the lower one for the case m congruent to 1 (4).

‡ The word "integer," unqualified, will be used in this paper to mean a quadratic integer.

§ Sommer, loc. cit., p. 40.

tegers satisfying conditions (1.) and (2.); for it is readily seen that, under these conditions, any integer of the field, $(a_1+b_1w)s+(a_2+b_2w)(t+w)$, may be expressed in the form $ls+n(t+w)$, l and n being rational integers.

The ideal conjugate to $(s, t+w)$, is, in canonic form,

$$\begin{cases} (s, s-t+w) \\ (s, s-t-1+w). \end{cases}$$

From conditions (1.) and (2.) and well-known theorems in the theory of rational integers, it follows that, for a given prime p not a factor of the discriminant of the field $\begin{pmatrix} d=4m \\ d=m \end{pmatrix}$, there are two canonic ideals $(p, t+w)$, or none, according as

$$\begin{cases} \left(\dfrac{m}{p}\right)=1 \text{ or } -1 \\ \left(\dfrac{m}{4p}\right)=1 \text{ or } -1 \end{cases}$$

When there are two, they are conjugate. If p is a factor of d, there is always one and only one ideal $(p, t+w)$. It is self-conjugate; and $t=0$ except in the two cases,

$$\text{(1.) } m\equiv 1 \ (4), \text{ when } t=\frac{p-1}{2},$$
$$\text{and (2.) } m\equiv 3 \ (4) \text{ and } p=2, \text{ when } t=1.$$

For any given rational integer s, there will be ideals of the form $(s, t+w)$ if and only if m is a quadratic remainder for each prime factor of s. If there are any such ideals, there will be just 2^r where r is the number of *distinct* prime factors of s which are not factors of d.

MULTIPLICATION.

Consider the product $(p, t_1+w)(p, t_2+w)$, p being a rational prime not a factor of d. Either these ideals are conjugate, in which case their product is the principal ideal $p(1, w)$, or else $t_1=t_2$ and the product is the square $(p, t_1+w)^2$. If $(p, t_1+w)^2=(s, t+w)$, s must be a number of $(p, t+w)$* and must therefore be divisible by p. Also, since p^2 is a number of $(s, t+w)$, s must be a factor of p^2. Hence s is either p or p^2. If $s=p$, then $(p, t_1+w)^2$ is (p, t_1+w) or its conjugate $(p, p-t_1+w)$.† The

* If one ideal is a factor of another, then every integer of the second is an integer of the first: cf. Sommer, loc. cit., p. 46.

† The argument is given for the case m not congruent to 1 (4). A very similar argument disposes of the case m congruent to 1 (4).

first supposition is trivial, being possible only for $(p,\ t_1+w)=(1,\ w)$. If $(p,\ t_1+w)^2=(p,\ p-t_1+w)$, then $p-t_1+w$ would be an integer of the ideal $(p,\ t_1+w)$. This could only be true if p were a factor of $2t_1$; and since $p\neq 2$ and $p>t_1$, it is impossible. Hence $s=p^2$, and t is uniquely determined by the conditions

$$\begin{cases} t^2\equiv m(p^2) \\ (2t+1)^2\equiv m(4p^2) \end{cases}$$
$$t\equiv t_1\,(p)$$
$$\text{and}\quad 0 \leqq t<p^2.$$

The condition $t\equiv t_1\,(p)$ must be true because pt_1+pw must be an integer of the product ideal, and hence there must be rational integers l and n such that

$$pt_1+pw=lp^2+n(t+w)$$

and it is evident that $n=p$ and $l=\dfrac{t_1-t}{p}$.

Similarly, it may be shown that

$$(p,\ t_1+w)^n=(p^n,\ t+w),$$

t being uniquely determined by the conditions

$$\begin{cases} t^2\equiv m(p^n) \\ (2t+1)^2\equiv m(4p^n) \end{cases}$$
$$t\equiv t_1\,(p)$$
$$0 \leqq t<p^n.$$

If q is a prime factor of d, then $(q,\ t+w)$ is self-conjugate; $(q,\ t+w)^2=q(1,\ w)$, $(q,\ t+w)^{2n}=q^n(1,\ w)$, and $(q,\ t+w)^{2n+1}=q^n(q,\ t+w)$.

Consider next the product $(s_1,\ t_1+w)(s_2,\ t_2+w)$ where s_1 and s_2 are relative primes. If the product is $(s,\ t+w)$, s must be an integer of both the ideals $(s_1,\ t_1+w)$ and $(s_2,\ t_2+w)$, and hence must be divisible by both s_1 and s_2, and therefore by their product s_1s_2. But s_1s_2 is an integer of the ideal $(s,\ t+w)$, and hence is divisible by s. Therefore $s=s_1s_2$, and t is uniquely determined by the conditions

$$\begin{cases} t^2\equiv m(s_1s_2) \\ (t2+1)^2\equiv m(4s_1s_2) \end{cases}$$

$$t \equiv t_1 (s_1)$$
$$t \equiv t_2 (s_2)$$
$$0 \leqq t < s_1 s_2.$$

Consider the ideal $(s, t+w)$, and let s_1 be any factor (prime or not) of s. Determine t_1 by the conditions $t_1 \equiv t(s_1)$ and $0 \leqq t < s_1$. Then it may be readily shown that every integer of the ideal $(s, t+w)$ is also an integer of the ideal (s_1, t_1+w), and hence (s_1, t_1+w) is a factor of $(s, t+w)$. We can then find a prime ideal factor of $(s, t+w)$ for every prime factor of s; and if we multiply these prime factors together by the laws shown above, their product will evidently be $(s, t+w)$. It follows then that *the ideal* $(s, t+w)$ *has a prime ideal factor for every prime factor of* s, *and that it has no other factors.*

Consider now the general product of $r_1(s_1, t_1+w)$ and $r_2(s_2, t_2+w)$, and let it be written $r_1 r_2\{r(s, t+w)\}$. In general, s_1 and s_2 will contain some prime factors which are factors of d, and some which are not; also some prime factors common to both s_1 and s_2, and some appearing only in one of the s's. Let the factors not in d be denoted by p's, and those in d by q's; and let the factors common to s_1 and s_2 be indicated by a bar thus, $\bar{p}$, $\bar{q}$. We may then write

$$s_1 = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots q_1 \, q_2 \ldots \bar{p}_1^{\beta_1} \bar{p}_2^{\beta_2} \ldots \bar{q}_1 \, \bar{q}_2 \ldots$$

$$\text{and } s_2 = p_{h+1}^{\alpha_{h+1}} p_{h+2}^{\alpha_{h+2}} \ldots q_{k+1} \, q_{k+2} \ldots \bar{p}_1^{\gamma_1} \bar{p}_2^{\gamma_2} \ldots \bar{q}_1 \, \bar{q}_2 \ldots$$

(q's may not occur to powers higher than the first).

Every factor p^{α} or q not common to both s_1 and s_2 will be a factor of s; and will contribute, for the determination of t, the condition

$$t \equiv t_1 \text{ or } t_2 \ \ (p \text{ or } q) \tag{3.}$$

Every $\bar{q}$ will be a factor of r, and will not appear as a factor in s.

For each $\bar{p}$ we first determine whether $t_1 \equiv t_2$ $(\bar{p})$ or t_1 not congruent to t_2 $(\bar{p})$. Those $\bar{p}$'s which are in the second class we will denote by a double bar $\bar{\bar{p}}$. For $\bar{p}$'s for which the congruence holds, $\bar{p}^{\beta+\gamma}$ will be a factor of s, $\bar{p}$ will not appear in r, and we will have the condition

$$t \equiv t_1 \equiv t_2 \ \ (\bar{p}) \tag{4.}$$

For a $\bar{\bar{p}}$, let δ be the smaller of the numbers β and γ. Then $\bar{\bar{p}}^{\delta}$ will be a factor of r, $\bar{\bar{p}}^{|\beta-\gamma|}$ will be a factor of s, and we will have

$$
\begin{aligned}
&t \equiv t_1 \ (\bar{\bar{p}}), \text{ if } \beta > \gamma \\
&\text{or } t \equiv t_2 \ (\bar{\bar{p}}), \text{ if } \gamma > \beta
\end{aligned}
\qquad (5.)
$$

The factors thus determined will make up r and s, and t will finally be uniquely determined by the condition

$$
\begin{cases} t^2 \equiv m \ (s) \\ (2t+1)^2 \equiv m \ (4s) \end{cases} \qquad (6.)
$$

together with conditions (3.), (4.), and (5.) above. Hence the product of $r_1(s_1,\ t_1+w)$ and $r_2(s_2,\ t_2+w)$ may be written $r_1 r_2 r(s,\ t+w)$, in which

$$r = \bar{q}_1\ \bar{q}_2 \dots \bar{\bar{p}}_1^{\delta_1}\ \bar{\bar{p}}_2^{\delta_2} \dots$$

$$s = p_1^{\alpha_1}\ p_2^{\alpha_2} \dots q_1\ q_2 \dots p_{h+1}^{\alpha h+1}\ p_{h+2}^{\alpha h+2} \dots q_{k+1}\ q_{k+2} \dots \bar{p}_1^{\beta_1+\gamma_1}\ \bar{p}_2^{\beta_2+\gamma_2} \dots \bar{\bar{p}}_1^{|\beta_1-\gamma_1|}\ \bar{\bar{p}}_2^{|\beta_2-\lambda_2|} \dots$$

and t is given by the conditions (3.)...(6.)

Examples. Consider the product $(399,\ 182+\sqrt{7})(378,\ 175+\sqrt{7})$. Here $d=28$, $s_1=399=19.3.7$, $s_2=378=2.3^3.7$, $s=19.2.3^2$; $t\equiv 175(2)$, $t\equiv 175(3)$, $t\equiv 182(19)$, $t^2\equiv 7(19.2.3^2)$, and $0 \overline{\leqq} t < (19.2.3^2)$, which makes $t=103$; $r=7.3$. Hence the product is $21(342,\ 103+\sqrt{7})$.

Consider $(120,\ 43+w)(700,\ 91+w)$ in the field $k(\sqrt{[-111]})$, $m\equiv 1(4)$, $w=\dfrac{1+\sqrt{[-111]}}{2}$, $d=-111$. Here $s=3.7.2^5.5$, $r=5$, and $t=1771$ from the conditions $t\equiv 43\equiv 91(2)$, $t\equiv 43(3)$, $t\equiv 91(5)$, $t\equiv 91(7)$, $(2t+1)^2\equiv -111(13440)$, giving the product $5(3380,\ 1771+w)$.

Canonic Form of the Principal Ideal Corresponding to an Irrational Integer.

The principal ideal corresponding to the integer $\alpha+\beta w$, α and β being rational integers prime to each other, may be put into canonic form by taking s as the norm of $\alpha+\beta w$, *i. e.*,

$$
s = \begin{cases} \alpha^2 - \beta^2 m \\ \alpha^2 + \alpha\beta - \beta^2 \dfrac{m-1}{4}. \end{cases}
$$

Then, for m not congruent to 1 (4), find a and b such that $a\beta + b\alpha = 1$, and hence $(a+bw)(\alpha+\beta w) = a\alpha + b\beta + w$, and we may take $t \equiv a\alpha + b\beta m(s)$. For

the case $m \equiv 1$ (4), find a and b such that $(a+b)\beta + b\alpha = 1$, and take $t \equiv a\alpha + b\beta\frac{m-1}{4}(s)$.

But, given an ideal in canonic form, it is not readily determined whether it is or is not a principal ideal; and hence we look for the necessary and sufficient conditions that a given ideal $(s, t+w)$ may be the principal ideal corresponding to some integer $\alpha+\beta w$. Consider the relation

(7.) $ls+nt+nw=(a+bw)(\alpha+\beta w)$, l, n, a, b, α, and β all rational integers.

Evidently $(s, t+w)$ will be a principal ideal if, and only if, we can find α and β such that

(1.) When a and b are arbitrarily assigned, l and n can be found to satisfy (7.); and

(2.) When l and n are arbitrarily assigned, a and b can similarly be found.

For simplicity consider the case m not congruent to 1 (4). Equating rational and irrational parts of (7.) we have

$$n=b\alpha+a\beta$$
$$l=\frac{a(\alpha+\beta t)+b(\beta m-\alpha t)}{s},$$

and if l is to be an integer for all values of a and b, we must have

$$\alpha-\beta t\equiv 0 \ (s) \qquad (8.)$$
$$\beta m-\alpha t\equiv 0 \ (s). \qquad (9.)$$

Again,
$$a=\frac{-l\alpha s-n(\beta m-\alpha t)}{\alpha^2-\beta^2 m}$$
and
$$b=\frac{l\alpha s+n(\beta-\beta t)}{\alpha^2-\beta^2 m}$$

and if a and b are to be integers for all values of l and n, we must have

$$\alpha s\equiv 0 \ (\alpha^2-\beta^2 m) \qquad (10.)$$
$$\beta s\equiv 0 \ (\alpha^2-\beta^2 m) \qquad (11.)$$
$$\alpha-\beta t\equiv 0 \ (\alpha^2-\beta^2 m) \qquad (12.)$$
$$\beta m-\alpha t\equiv 0 \ (\alpha^2-\beta^2 m) \qquad (13.)$$

If (8.) is true, then $\alpha t-\beta t^2\equiv 0$ (s), and since $t^2\equiv m$ (s) we must have $\alpha t-$

$\beta m \equiv 0$ (s). Hence (8.) includes (9.). Again, if α contained any factor of $\alpha^2-\beta^2 m$, β would also have to contain it; and since α and β are prime to each other, this is impossible. Hence (10.) and (11.) reduce to $s\equiv 0$ $(\alpha^2-\beta^2 m)$, and this in turn brings (12.) and (13.) under (8.). Hence our six conditions reduce to two, namely,

$$\alpha-\beta t\equiv 0 \ (s) \tag{8.}$$

$$\text{and } s\equiv 0 \ (\alpha^2-\beta^2 m) \tag{14.}$$

Moreover, since $\alpha-\beta t\equiv 0$ (s), we have $\alpha t-\beta t^2\equiv 0$ (s), and hence $\alpha^2-\beta^2 m\equiv 0$ (s). But this, together with (14.), gives us the equation

$$\pm s=\alpha^2-\beta^2 m \tag{15.}$$

Similarly for the case $m\equiv 1$ (4), we find that the conditions redvce to (8.) and the equation

$$\pm s=\alpha^2+\alpha\beta-\beta^2\frac{m-1}{4} \tag{16.}$$

Hence the necessary and sufficient condition that $(s, t+w)$ should be a principal ideal is that it should be possible to find rational integers α and β to satisfy equation (15.) or (16.) and congruence (8.).

If s is a prime number, the equation alone is sufficient.

As a special case, the conditions ars evidently fulfilled if the norm of $t+w$, t^2-w^2, is equal to s; in which case $(s, t+w)$ is the principal ideal corresponding to $t+w$.

Equation (15.), or (16.), gives the necessary condition for a principal ideal that $\left(\frac{\pm s}{m}\right)=1$, or $\left(\frac{\pm 4s}{m}\right)=1$, while for any ideal whatever we must have

$$\begin{cases} \left(\frac{m}{s}\right)=1. \\ \left(\frac{m}{4s}\right)=1. \end{cases}$$

The necessary and sufficient condition in the form to which we have reduced it is of little practical value as a test if $m>0$. For $m<0$ it may be useful.